

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,)
)
)
Plaintiff,)
)
)
v.)
)
TWENTY-FOUR CRYPTOCURRENCY	Civil Action No. 19-cv-3098
ACCOUNTS)
)
Defendants.)
)
)

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America, by and through the United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture *in Rem* against the defendant properties, namely: twenty-four cryptocurrency accounts (the “Defendant Properties”), which are listed in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions:

THE DEFENDANT PROPERTIES

1. The Defendant Properties are comprised of miscellaneous financial instruments (listed in Attachment A). The Defendant Properties are in the possession of the United States.

NATURE OF ACTION AND THE DEFENDANTS IN REM

2. This *in rem* forfeiture action arises out of an investigation by the Internal Revenue Service – Criminal Investigation’s Cyber Crimes Unit (“IRS-CI”) and Homeland Security Investigations (“HSI”) into a child pornography website called Welcome To Video. Co-conspirator users of Welcome To Video have knowingly and willfully conspired with others and

acted individually to: launder monetary instruments, in violation of 18 U.S.C §1956(a)(2) and (h); receive or distribute any visual depiction which contains materials depicting a minor engaging in sexually explicit conduct, which have been mailed or shipped or transported by computer in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); possess and access with intent to view a depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); distribute and be in receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1); and possess and access a device with intent to view child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2). These individuals laundered the Defendant Properties to procure content in violation of the above statutes.

3. The Defendant Properties are subject to forfeiture pursuant to 18 U.S.C. § 2254, as property used or intended to be used to commit or to promote the commission of the above offenses. The Defendant Properties are also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in, or traceable to, a financial transaction in violation of 18 U.S.C § 1956.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355. These statutes confer original jurisdiction to district courts of all civil actions, suits, or proceedings commenced by the United States and any action for the forfeiture of property incurred under any act of Congress.

5. Venue is proper pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred within the District of Columbia. Venue is also proper pursuant to 28 U.S.C. § 1395(c) because the Defendant Properties are held in the District of Columbia.

FACTS GIVING RISE TO FORFEITURE

I. Definition of Terms

6. Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address attached to computers on the internet that, when assigned, properly directs internet traffic. Tor can be accessed by installing freely available Tor software. Tor relays only the IP address of the last relay computer (the "exit node"), masking the user's actual IP address. With Tor, users can operate a special type of website, called a "hidden services" website, which uses web addresses comprised of 16 algorithm-generated characters followed by the suffix ".onion." Hidden service websites have system administrator(s) who oversee their operation.

7. Bitcoin ("BTC") is a type of virtual currency, or "cryptocurrency," which is circulated over the Internet. BTC is not issued by a government, bank, or company, but rather is controlled through computer software. BTC is generally sent and received using a BTC "address," which is like a bank account number represented by a case-sensitive string of numbers and letters. Each address is controlled through the use of a unique private "key," akin to a password. Users can operate numerous addresses at a given time, with the option to use a unique address for every transaction. BTC fluctuates in value. As of March 5, 2018, one BTC was worth approximately \$11,573.00. Typically, users purchase BTC from a BTC virtual-currency exchange, a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Though little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself, virtual currency exchanges are required by U.S. law to collect customers' identifying information and verify their clients' identities. BTC can be sent to another address by a user via a transaction announcement, signed with their key. Once verified, the

transaction is added to the “blockchain,” a decentralized, public ledger that logs every BTC transaction. Blockchain analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity, and allow the identification of BTC addresses that are involved in transacting with the same addresses.

8. The Defendant Properties include U.S. Dollars, BTC, and other forms of cryptocurrency (*e.g.*, Litecoin (LTC), Ethereum (ETH), Dogecoin (DOGE), Bitcoin Cash (BCH), etc.). These other forms of cryptocurrency exist and operate in a manner similar to BTC, and just like BTC, fluctuate in value over the course of time.

II. Welcome To Video Website

9. Welcome To Video was a Tor network-based child-pornography website, which began operating at least in or about June 2015. Welcome To Video hosted and distributed image and video files depicting child pornography. The upload page on Welcome To Video stated: “Do not upload **adult porn** [emphasis added by the website].”

10. On or about February 8, 2018, Welcome To Video indicated on its download page details that its users had downloaded files from Welcome To Video more than a million times.

11. On or about March 5, 2018, Welcome To Video’s server had over 200,000 unique video files, which totaled approximately eight terabytes of data. As files were uploaded by users, Welcome To Video compared the video’s hash to previously uploaded videos to prevent the duplication of videos. Each video had a title, a description (if included by the uploader), “tags” with further descriptions of the video, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

12. The video search page of Welcome To Video listed keyword search terms and the number of videos associated with each keyword. On or about February 8, 2018, some of the top

keyword search terms and the associated approximate videos included “PTHC,” “PEDO,” “%2yo,” “%4yo,” and “incest.”

- a. “PTHC” is an abbreviation for “preteen hardcore.”
- b. “Pedo” is an abbreviation for “pedophile.”
- c. “%2yo” is an abbreviation for “2 year old.”
- d. “%4yo” is an abbreviation for “4 year old.”

13. To access the site, customers created a free account on Welcome To Video by creating a username and password, but supplied no other identifiable information such as an email address. Once a customer had an account, they could browse picture previews of videos depicting child pornography that were available for download.

14. In order to download videos from Welcome To Video, customers redeemed “points.” Points could be obtained by: (1) uploading videos depicting child pornography; (2) referring new customers to Welcome To Video; (3) paying 0.03 BTC (approximately \$352.59 as of March 5, 2018) for a “VIP” account, which lasted for six months and purportedly allowed unlimited downloads; and/or (4) paying for points incrementally (*i.e.*, 0.02 bitcoin for 230 points). Points were not transferable to any other website or application. Once BTC were sent to Welcome To Video, they could not be refunded or redirected. Points obtained by the payment of BTC could only be used for downloading videos. Once a user uploaded videos depicting child pornography to Welcome To Video, the uploader was unable to delete the video. However, the administrator retained access to these videos and all BTC accumulated by Welcome To Video.

15. Welcome To Video directed customers to particular BTC exchanges to make payments, including an exchange in the United States. Welcome To Video assigned a unique BTC

address for each Welcome To Video customer account to receive payments and assign points appropriately. There were over 1.3 million BTC addresses set up by Welcome To Video.

16. Law enforcement gathered a list of thousands of unique BTC addresses associated with Welcome To Video. This list included an undercover agent's BTC address which Welcome To Video assigned to the undercover agent when the undercover agent created an account on Welcome To Video.

17. From in or about June 2015 to on or about March 8, 2018, Welcome To Video received at least 420 BTC through at least 7,300 transactions worth over \$370,000.00 at the time of the respective transactions. Transactions originated in numerous countries, including the United States, the United Kingdom, and South Korea.

18. On multiple occasions, an agent acting in an undercover capacity paid BTC to Welcome To Video and used the website to download child pornography video files while in Washington, D.C. These child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Specifically, those video files contained the following:

a. File name [REDACTED] with the video tag description [REDACTED] depicted a child, approximately ten years old, and an adult male inserting his penis into the child's mouth and anus. Welcome To Video customers downloaded this video 957 times;

b. File name [REDACTED] with the video tag description [REDACTED] [REDACTED] depicted a female child approximately three years old. The child is nude and bound with her legs spread apart so that her genitalia is visible. An adult male urinates on her. Welcome To Video customers downloaded this video 219 times;

c. File name [REDACTED] with the video tag description [REDACTED]
[REDACTED] depicted a female toddler, approximately two or three years old. An adult male inserted his penis inside of the anus of the female toddler. Welcome To Video customers downloaded this video 369 times;

d. File name [REDACTED] with the video tag description [REDACTED]
[REDACTED] depicted an infant, approximately six months old. An adult male inserted his penis inside the mouth and anus of the infant. Welcome To Video customers downloaded this video 113 times;

e. File name [REDACTED] with the video tag description [REDACTED]
[REDACTED] depicted a male child, approximately ten years old. An adult male inserted his penis into the child's mouth and anus while in a shower. Welcome To Video customers downloaded this video three times; and

f. Finally, file name [REDACTED] with the video tag description [REDACTED]
[REDACTED] depicted a female child, approximately eight years old. An adult male inserted his penis into the child's anus. Welcome To Video customers downloaded this video 69 times.

III. Events Leading Up to the Seizure of Defendant Properties

19. On or about September 1, 2017, law enforcement reviewed the source code of Welcome To Video's homepage, which could be viewed by right-clicking on Welcome To Video in the Tor browser and selecting "View Page Source." In reviewing the source code, law enforcement discovered that Welcome To Video had failed to conceal its server's IP address. This IP address resolved to a telecommunications provider in South Korea. Subsequently the

investigation confirmed that this IP address was registered in the name of Jong Woo Son and that the address serviced his residence in South Korea.

20. On February 28, 2018, a federal magistrate judge in the United States District Court for the District of Columbia issued an arrest warrant for Jong Woo Son.

21. On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of Jong Woo Son in South Korea. Pursuant to the search, South Korean law enforcement seized Welcome To Video's server and associated electronic storage media from the bedroom of Jong Woo Son. U.S. law enforcement subsequently received a forensic image of the Welcome To Video server.

22. A review of the imaged data confirmed that Welcome To Video was hosted on the seized server. A review of a sample of the video files further corroborated that Welcome To Video was dedicated to the distribution of child pornography. The customer data generally identified which customer was associated with which BTC payment to Welcome To Video. A review of a sample of the payments to Welcome To Video cross-referenced against the username and download data from the server revealed that payments to Welcome To Video corresponded with the user downloading videos from Welcome To Video. A review of the forensic image of the server further revealed that certain Welcome to Video co-conspirators uploaded illicit content to the site.

23. On August 8, 2018, a federal grand jury in the District of Columbia indicted Jong Woo Son on various counts, including Conspiracy to Distribute Child Pornography, in violation of Title 18, United States Code, Sections 2252(a)(2) and (b)(1). *See* 1:18-mj-00243 (DAF) (Sealed).

IV. The Defendant Properties

24. Analyzing the blockchain revealed BTC addresses that laundered BTC to Welcome To Video from accounts hosted at BTC Exchange 1, BTC Exchange 2, and BTC Exchange 3, (collectively, the “BTC Exchanges”). The BTC Exchanges are all cryptocurrency exchanges offering services to customers worldwide include storing cryptocurrency in online “wallets.”

25. Based on the investigation as described above, law enforcement discovered the below accounts at the BTC Exchanges, which comprise the Defendant Properties. Law enforcement previously seized these twenty-four accounts pursuant to a judicially-authorized seizure warrant.

a) BTC Exchange 1

1. BTC Exchange 1 account **5185e2c6b3bd3de60e00002a** – From approximately August 16, 2015 to July 9, 2016, this account laundered BTC nine times to a BTC address controlled by Welcome to Video totaling approximately 0.91 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “gat0rs,” who downloaded at least 219 videos from Welcome To Video. Further, blockchain analysis revealed that this account also laundered BTC to darknet markets, including Agora, AlphaBay, Evolution, and Silk Road, which sold drugs, stolen information, and other illicit products.
2. BTC Exchange 1 account **5652a83e6f4be24bf9000110** – On or about February 5, 2018, this account laundered approximately 0.01035562 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “jaclist2010,” who downloaded at least nine videos from Welcome To Video.
3. BTC Exchange 1 account **559715bd61373556e00000ae** – On or about July 10, 2015, this account laundered approximately 0.10 BTC to a BTC address controlled

by Welcome To Video. The BTC transaction had a memo of “UserName: loki354.” User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “loki354,” who downloaded at least six videos from Welcome To Video.

4. BTC Exchange 1 account **58760323ee243500a3067f85** – On or about August 25, 2017, and September 6, 2017, this account laundered two payments to a BTC address controlled by Welcome To Video totaling approximately 0.02203612 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “poopman420k,” who downloaded at least 205 videos from Welcome To Video.
5. BTC Exchange 1 account **56454cd5399d4a00f00001ae** – On or about November 13, 2015 this account laundered approximately 0.25 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “mg2005,” who downloaded at least four videos from Welcome To Video, and uploaded at least one video, which had the title of [REDACTED] [REDACTED] to Welcome To Video.
6. BTC Exchange 1 account **524c41b07f435f428400005a** – On or about October 20, 2015, this account laundered approximately 0.18 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “jor1092,” who downloaded an approximate total of 52,592.7 MBs worth of videos (the maximum for a six month VIP account – which allowed another user to download approximately 676 videos) from Welcome To Video. Further, blockchain analysis revealed that this account also laundered BTC to darknet markets, including Agora and Evolution, which sold drugs, stolen information, and other illicit products.
7. BTC Exchange 1 account **563443739ac69f3b29000170** – On or about December 9, 2015, this account laundered approximately 0.10 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of

the server revealed the above listed BTC payment was linked to Welcome To Video username “franky77,” who downloaded an approximate total of 52,592.7 MB worth of videos (the maximum for a six month VIP account – which allowed another user to download approximately 676 videos) from Welcome To Video. Further, blockchain analysis revealed that this account also laundered BTC to darknet markets, including Hansa and AlphaBay, which sold drugs, stolen information, and other illicit products.

8. BTC Exchange 1 account **5a4fab5fd24e170544892941** – On or about January 21, 2018, this account laundered approximately 0.00133308 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “insipity,” who downloaded at least 98 videos from Welcome To Video.
9. BTC Exchange 1 account **5676f8ba7d98e545080000b8** – On or about September 3, 2017 and November 23, 2017, this account laundered two payments to a BTC address controlled by Welcome To Video totaling approximately 0.04141252 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “qtnvomaz,” who downloaded at least 310 videos from Welcome To Video.
10. BTC Exchange 1 account **5687df5a4b12f73aa50000c0** – On or about February 6, 2017, and August 13, 2017, this account laundered two payments to a BTC address controlled by Welcome To Video totaling approximately 0.24049414 BTC. One of the BTC transactions had a memo of “I forgot my user pass so signed up again. desinnude [sic] Welcome1.” That is, the account owner was indicating that he forgot his password for his account on Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “desinude.” This account also laundered approximately 1.05 BTC on or about January 8, 2016 to a second BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the second BTC address was linked to Welcome To Video username “winkit,” who downloaded at least 113 videos from Welcome To Video.

11. BTC Exchange 1 account **55f1718c2289a067b50001fa** – On or about September 18, 2015, this account laundered two payments to a BTC address controlled by Welcome To Video totaling approximately 0.34 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “asd8973,” who downloaded an approximate total of 52,592.7 MBs worth of videos (the maximum for a six month VIP account – which allowed another user to download approximately 676 videos) from Welcome To Video.
12. BTC Exchange 1 account **55a4403965373100d7000165** – On or about July 18, 2015, this account laundered approximately 0.29 BTC to a BTC address controlled by Welcome To Video. The BTC transaction had the memo of “VIP for thalaw plz and thanks.” User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “thalaw,” who purchased a six month VIP account (a six month VIP account allowed another user to download approximately 676 videos). Further, blockchain analysis revealed that this account also laundered BTC to darknet markets, including Agora, that sold drugs, stolen information, and other illicit products.
13. BTC Exchange 1 account **566a1a4495c0be0d1c000230** – On or about April 18, 2016, this account laundered approximately 0.02 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “m8te666.” This user also appeared on other known darknet and illicit sites which offered money laundering services and child pornography content.
14. BTC Exchange 1 account **55f974c78cc94d4d4b000244** – On or about September 18, 2015, this account laundered an approximate total of 0.45 BTC to a BTC address controlled by Welcome To Video. The BTC transaction had a memo that stated “0 BTC (X) user blinder.” User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “blinder,” who downloaded an approximate total of 52,592.7 MB worth

of videos (the maximum for a six month VIP account – which allowed another user to download approximately 676 videos) from Welcome To Video.

15. BTC Exchange 1 account **531e0828ead59cce4a000264** – Between October 11, 2015, and April 30, 2016, this account laundered four payments to four BTC addresses controlled by Welcome To Video totaling approximately 0.66 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video usernames “freepdc,” “detnews,” “lucytai,” and “freepdc4.” Users “freepdc” and “detnews” downloaded an approximate total of 52,592.7 MB worth of videos (the maximum for a six month VIP account – which allowed another user to download approximately 676 videos) from Welcome To Video. On or about October 23, 2017, law enforcement seized the account owner’s electronic media. On or about the morning of October 25, 2017, the account owner committed suicide at his Washington, D.C. residence. A search of the account owner’s media revealed numerous files depicting child pornography. Further, blockchain analysis revealed that the BTC account also laundered BTC to darknet markets, including Agora and Dream, which sold drugs, stolen information, and other illicit products.

16. BTC Exchange 1 account **583c85d54d3af20217519752** – Between November 28, 2016, and April 26, 2017, this account laundered three payments to a BTC address controlled by Welcome To Video totaling approximately 0.13049720 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “karmacowboy,” who downloaded at least 78 videos from Welcome To Video.

17. BTC Exchange 1 account **558ac736316131095b0001a4** – Between July 20, 2015, and May 22, 2017, this account laundered 13 payments to a BTC address controlled by Welcome To Video totaling approximately 1.12 BTC. User data obtained from the forensic image of the server revealed the above listed BTC payments were linked to Welcome To Video username “trincaps2,” who downloaded at least 676 videos (with an approximate total size of 52,592.7 MB worth of videos, which was the maximum for a six month VIP account) from Welcome To Video.

a. On June 15, 2018, law enforcement executed a search warrant of the account owner's residence in relation to this investigation. The search revealed child pornography located on the account owner's electronic devices. The account owner was subsequently arrested on an indictment charging possession and receipt of child pornography.

18. BTC Exchange 1 account **573808d68fdf8333f300002a** – On or about May 21, 2016, this account laundered approximately 0.090 BTC to a BTC address controlled by Welcome To Video. The BTC transaction had the memo of “I am user gregorystill.” User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “gregorystill.” Other transaction memos for payments from this account included “suscripcpm [sic] naughty” and “I [sic] buy a 1 month suscription [sic].”

- a. This account also laundered 0.012 BTC with the memo “it is the buy for you” to a cluster of BTC addresses which then laundered BTC to Welcome To Video. The recipient of this payment previously sent BTC to the account “pteen,” (which is an abbreviation for “preteen”) at Welcome To Video.
- b. This BTC cluster sold child pornography, based on a review of other payments to this clustered address. Specifically, the cluster received approximately 141 transactions during approximately two months. The cluster received payments from several exchanges, most of which then went to a bitcoin mixing service. Mixing services are companies, often on the darkweb, that mix all the payments received from numerous users together in order to conceal where the money comes from and where it goes.
- c. In summary the account owner opened his BTC Exchange 1 account on or about May 14, 2016, funded the account over the next few days then only sent four payments, one directly to Welcome To Video and three to a cluster that subsequently laundered BTC to Welcome To Video.

19. BTC Exchange 1 account **56d3b1cc9f49041768000086** – On or about December 6, 2016, and January 29, 2017, this account laundered two payments to a BTC address controlled by Welcome To Video totaling approximately 0.090 BTC. User data obtained from the forensic image of the server revealed the above listed BTC

payments were linked to Welcome To Video username “hamburger,” who downloaded at least 130 videos from Welcome To Video.

- a. On August 16, 2018, law enforcement executed a search warrant at the account owner’s residence in relation to this investigation and located child pornography on his electronic devices.

b) BTC Exchange 2

1. BTC Exchange 2 account **Francoca.87** – On or about May 27, 2017, this account laundered approximately 0.020 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “fsdfds465456,” who downloaded at least 15 videos from Welcome To Video.
2. BTC Exchange 2 account **ihackgeek** did not have a registered name or associated email address. The account had a phone number with an Eastern European country code and the IP log showed consistent access from Eastern Europe, namely Ukraine and Russia. The account only had one BTC transaction. On or about May 27, 2017, this account laundered approximately 0.0116 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “ihackgeek,” who downloaded at least 87 videos with an approximate total size of 9,286.5 MBs.
3. BTC Exchange 2 account **Um2541** did not have a registered name but had an associated email address and logins from IP addresses exclusively from South Korea. On or about August 31, 2017, this account laundered approximately 0.010 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “um2525,” who downloaded at least 81 videos from Welcome To Video.
 - a. The account owner subsequently asked law enforcement “if you stopped my account because I received a video on Deep Web.”

c) BTC Exchange 3

1. BTC Exchange 3 account **longhorn1** had no registered name, but had an associated email address and a phone number with an Austin, Texas area code. On or about April 26, 2016, this account laundered approximately 0.1808 BTC to a BTC address controlled by Welcome To Video. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “mexman16.”
 - a. This account also laundered 0.05 BTC to the same cluster of BTC addresses that laundered BTC to the account “pteen” at Welcome To Video.
 - b. This account also laundered 0.2508 BTC to a cluster of BTC address that sent approximately 0.48643035 BTC in 10 transactions to Welcome To Video. This second cluster sent a substantial portion of funds (approximately 1,000 BTC) to a darknet mixing service that openly advertises that it launders funds for anyone that wants to conceal their illicit payments.
2. BTC Exchange 3 account **culboy2012** had no registered name, but had an associated email address. On or about November 12, 2015, this account was created, funded in under 30 minutes, and within two hours the user laundered approximately 0.1308 BTC to a BTC address controlled by Welcome To Video. The account was never logged into again. User data obtained from the forensic image of the server revealed the above listed BTC payment was linked to Welcome To Video username “billvssharon.”

FIRST CLAIM FOR RELIEF
(18 U.S.C. § 2254)

26. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 25 above as if fully set forth herein.

27. The Defendant Properties were property, real or personal, used or intended to be used to commit or to promote the commission of a violation of 18 U.S.C. §§ 2252 and 2252A, and/or property traceable to such property

SECOND CLAIM FOR RELIEF
(18 U.S.C. § 981(A)(1)(A))

28. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 25 above as if fully set forth herein.

29. The Defendant Properties were involved in a conspiracy to launder and the laundering of monetary instruments intended to promote the carrying on of a specified unlawful activity, that is, 18 U.S.C. § 2252 and 18 U.S.C. § 2252A (relating to child pornography) where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct.

30. As such, the Defendant Properties are subject to forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(A), as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Properties as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that a warrant of arrest *in rem* issue according to law; that judgment be entered declaring that the Defendant Properties be forfeited for disposition according

to law; and that the United States of America be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: October 16, 2019

Respectfully submitted,

JESSIE K. LIU, D.C. Bar No. 472845
United States Attorney

By: _____/s/
ZIA M. FARUQUI, D.C. Bar No. 494990
Lindsay Suttenberg, D.C. Bar No. 978513
Youli Lee, D.C. Bar No. 4064028
Assistant United States Attorneys
555 Fourth Street, N.W.
Washington, D.C. 20530
(202) 252-7117 (Faruqui)

/s/
C. ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Ave NW
Washington, D.C. 20005
(202) 514-1026

Attorneys for the United States of America

VERIFICATION

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 16th day of October, 2019.

/s/
Christopher Janczewski
Special Agent
Internal Revenue Service

Attachment A

BTC		USD	EUR	BTC	BCH	ETH	LTC
Exchange	Account						
1	5185e2c6b3bd3de60e00002a						
1	5652a83e6f4be24bf9000110						
1	559715bd61373556e00000ae						
1	58760323ee243500a3067f85						
1	56454cd5399d4a00f00001ae						
1	524c41b07f435f428400005a						
1	563443739ac69f3b29000170						
1	5a4fab5fd24e170544892941						
1	5676f8ba7d98e545080000b8						
1	5687df5a4b12f73aa50000c0	995.71	18.05	4.90476894	3.91310093	6.1740011	7.77515352
1	55f1718c2289a067b50001fa						
1	55a4403965373100d7000165						
1	566a1a4495c0be0d1c000230						
1	55f974c78cc94d4d4b000244						
1	531e0828ead59cce4a000264						
1	583c85d54d3af20217519752						
1	558ac736316131095b0001a4						
1	573808d68fdf8333f300002a						
1	56d3b1cc9f49041768000086						
2	Francoca.87	3,187.66					
2	ihackgeek	1,680.72					
2	Um2541	32,522.95					
3	Culboy2012			0.31875905			
3	Longhorn1			0.08619007			
		\$ 38,387.04	18.05	5.30971806	3.91310093	6.1740011	7.77515352

CIVIL COVER SHEET

JS-44 (Rev. 5/12 DC)

I. (a) PLAINTIFFS		DEFENDANTS	
(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF _____ (EXCEPT IN U.S. PLAINTIFF CASES)		COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____ (IN U.S. PLAINTIFF CASES ONLY) NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED	
(c) ATTORNEYS (FIRM NAME, ADDRESS, AND TELEPHONE NUMBER)		ATTORNEYS (IF KNOWN)	
II. BASIS OF JURISDICTION (PLACE AN x IN ONE BOX ONLY)		III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) FOR DIVERSITY CASES ONLY!	
<input type="radio"/> 1 U.S. Government Plaintiff <input type="radio"/> 3 Federal Question (U.S. Government Not a Party)		PTF DFT Citizen of this State <input type="radio"/> 1 <input type="radio"/> 1 Incorporated or Principal Place of Business in This State <input type="radio"/> 4 <input type="radio"/> 4	
<input type="radio"/> 2 U.S. Government Defendant <input type="radio"/> 4 Diversity (Indicate Citizenship of Parties in item III)		Citizen of Another State <input type="radio"/> 2 <input type="radio"/> 2 Incorporated and Principal Place of Business in This State <input type="radio"/> 5 <input type="radio"/> 5	
		Citizen or Subject of a Foreign Country <input type="radio"/> 3 <input type="radio"/> 3 Foreign Nation <input type="radio"/> 6 <input type="radio"/> 6	

IV. CASE ASSIGNMENT AND NATURE OF SUIT

(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

<input type="radio"/> A. <i>Antitrust</i> 410 Antitrust	<input type="radio"/> B. <i>Personal Injury/Malpractice</i> 310 Airplane 315 Airplane Product Liability 320 Assault, Libel & Slander 330 Federal Employers Liability 340 Marine 345 Marine Product Liability 350 Motor Vehicle 355 Motor Vehicle Product Liability 360 Other Personal Injury 362 Medical Malpractice 365 Product Liability 367 Health Care/Pharmaceutical Personal Injury Product Liability 368 Asbestos Product Liability	<input type="radio"/> C. <i>Administrative Agency Review</i> 151 Medicare Act <u>Social Security</u> 861 HIA (1395ff) 862 Black Lung (923) 863 DIWC/DIWW (405(g)) 864 SSID Title XVI 865 RSI (405(g)) <u>Other Statutes</u> 891 Agricultural Acts 893 Environmental Matters 890 Other Statutory Actions (If Administrative Agency is Involved)	<input type="radio"/> D. <i>Temporary Restraining Order/Preliminary Injunction</i> Any nature of suit from any category may be selected for this category of case assignment. *(If Antitrust, then A governs)*
--	---	---	--

 E. *General Civil (Other)* OR F. *Pro Se General Civil*

<u>Real Property</u> 210 Land Condemnation 220 Foreclosure 230 Rent, Lease & Ejectment 240 Torts to Land 245 Tort Product Liability 290 All Other Real Property	<u>Bankruptcy</u> 422 Appeal 27 USC 158 423 Withdrawal 28 USC 157 <u>Prisoner Petitions</u> 535 Death Penalty 540 Mandamus & Other 550 Civil Rights 555 Prison Conditions 560 Civil Detainee – Conditions of Confinement <u>Property Rights</u> 820 Copyrights 830 Patent 840 Trademark <u>Federal Tax Suits</u> 870 Taxes (US plaintiff or defendant) 871 IRS-Third Party 26 USC 7609	<u>Forfeiture/Penalty</u> 625 Drug Related Seizure of Property 21 USC 881 690 Other <u>Other Statutes</u> 375 False Claims Act 400 State Reapportionment 430 Banks & Banking 450 Commerce/ICC Rates/etc. 460 Deportation 462 Naturalization Application 465 Other Immigration Actions 470 Racketeer Influenced & Corrupt Organization	480 Consumer Credit 490 Cable/Satellite TV 850 Securities/Commodities/Exchange 896 Arbitration 899 Administrative Procedure Act/Review or Appeal of Agency Decision 950 Constitutionality of State Statutes 890 Other Statutory Actions (if not administrative agency review or Privacy Act)
---	---	--	--

<input type="radio"/> G. Habeas Corpus/2255 530 Habeas Corpus – General 510 Motion/Vacate Sentence 463 Habeas Corpus – Alien Detainee	<input type="radio"/> H. Employment Discrimination 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation)	<input type="radio"/> I. FOIA/Privacy Act 895 Freedom of Information Act 890 Other Statutory Actions (if Privacy Act)	<input type="radio"/> J. Student Loan 152 Recovery of Defaulted Student Loan (excluding veterans)
(If pro se, select this deck)		*(If pro se, select this deck)*	
<input type="radio"/> K. Labor/ERISA (non-employment) 710 Fair Labor Standards Act 720 Labor/Mgmt. Relations 740 Labor Railway Act 751 Family and Medical Leave Act 790 Other Labor Litigation 791 Empl. Ret. Inc. Security Act	<input type="radio"/> L. Other Civil Rights (non-employment) 441 Voting (if not Voting Rights Act) 443 Housing/Accommodations 440 Other Civil Rights 445 Americans w/Disabilities – Employment 446 Americans w/Disabilities – Other 448 Education	<input type="radio"/> M. Contract 110 Insurance 120 Marine 130 Miller Act 140 Negotiable Instrument 150 Recovery of Overpayment & Enforcement of Judgment 153 Recovery of Overpayment of Veteran's Benefits 160 Stockholder's Suits 190 Other Contracts 195 Contract Product Liability 196 Franchise	<input type="radio"/> N. Three-Judge Court 441 Civil Rights – Voting (if Voting Rights Act)
V. ORIGIN <input type="radio"/> 1 Original Proceeding <input type="radio"/> 2 Remand from State Court <input type="radio"/> 3 Remanded from Appellate Court <input type="radio"/> 4 Reinstated or Reopened <input type="radio"/> 5 Transferred from another district (specify) <input type="radio"/> 6 Multi-district Litigation <input type="radio"/> 7 Appeal to District Judge from Mag. Judge			
VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)			
VII. REQUESTED IN COMPLAINT	CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23	DEMAND \$ JURY DEMAND:	Check YES only if demanded in complaint YES NO
VIII. RELATED CASE(S) IF ANY	(See instruction)	YES NO	If yes, please complete related case form
DATE: _____	SIGNATURE OF ATTORNEY OF RECORD _____ /s/ Zia Faruqui _____		

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil cover sheet. These tips coincide with the Roman Numerals on the cover sheet.

- I.** COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.
- III.** CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.
- IV.** CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.
- VI.** CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.
- VIII.** RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should endure the accuracy of the information provided prior to signing the form.

CLERK'S OFFICE
UNITED STATES DISTRICT COURT

CO-931
New 3/78

**NOTICE OF DESIGNATION OF PENDING* RELATED CRIMINAL
CASE PURSUANT TO RULE 3-4, UNITED STATES DISTRICT
COURT FOR THE DISTRICT OF COLUMBIA**

Criminal Number: _____
(To be supplied by the Clerk)

NOTICE TO PROSECUTOR:

Pursuant to LCrR 57.12(a)(1) of this Court's Rules, you should prepare this form and submit it to the Clerk's Office along with the indictments in any related cases. One copy is needed for the Clerk's records, once for the Judge to whom the case is assigned, and one additional copy for each defendant. Therefore, in a one defendant case you should submit 3 copies, for a two defendant case you should submit 4 copies, etc. The Clerk will mail copies of this form to all defense counsel along with the arraignment notice.

NOTICE TO DEFENDANT:

Rule LCrR 57.12(b)(1) of this Court's Rules requires that any objection by the defendant to the related case designation shall be served on the U. S. Attorney and filed with the Clerk within 10 days after arraignment.

NOTICE TO ALL COUNSEL:

Rule LCrR 57.12(b)(3) requires, in part, that as soon as an attorney for a party becomes aware of the existence of a related case or cases, such attorney shall immediately notify in writing, the Judges on whose calendars the cases appear and shall serve such notice on counsel for all other parties.

The prosecutor will please complete the following:

1. Name of defendant: JONG WOO SON
2. Number of related case: 18-cr-0243
3. Name of Judge assigned to related case: Dabney L. Friedrich
4. Name of United States Court in which the related case is pending (if other than this Court): _____

5. Relationship of new case to related case: Common Parties _____

[Check appropriate box(es)]

(a) New case is a superseding information.

(b) More than one indictment is filed or pending against defendant.

(c) Prosecution against different defendant(s) arises from:
 a common wiretap
 a common search warrant
 activities which are a part of the same alleged criminal event or transaction

(*) A case is considered pending until a defendant has been sentenced. [Rule 3-4(a)(1)]